インターネット・アイデンティティとプライバシー～OpenID を中心にした考察

崎村 夏彦

2010/09/21

【概要】

インターネットでのやりとりが市民の生活に占める割合は年々大きくなっている。
必然的にネット上の人格である「インターネット・アイデンティティ」の重要性もあがってきているが、
その性質についてよく理解されないまま現実が進んでしまっているため
プライバシー等様々な問題を生んでいる。
本講演では、インターネット・アイデンティティの定義、性質からはじめ、今後の方向性について展望する。

キーワード:アイデンティティ、プライバシー、同意フレームワーク、Governance as a Platform,

アイデンティティ（自我同一性）

自我は社会的発達の過程において多くの他者や集団や社会の価値・規範・役割期待などを取得するが，その結果，それぞれの他者・集団・社会に対する複数の「~としての自分」と，それぞれの他者・集団・社会と共通する観点・一般化された他者の観点を獲得する。

個人はそれぞれの状況に応じて一定の社会的役割を果たすことによって自分の自我を確認し検証する。

例えば，

- *長男（長女）としての自分，*
- *友人としての自分，*
- *親としての自分，*
- *男（女）としての自分，*
- *会社の一員としての自分，*
- *日本人としての自分*

などである。

このようなそれぞれの「~としての自分」を選択しつつ行為するが，これら複数の「~としての自分」の同一性を統合し，秩序づけ組織化する普遍的統合的自我の連続性・斉一性・普遍性を自我同一性（ego-identity）と，エリクソンは呼んでいる。それは，個人独自の存在であることの証明である。（越井郁郎）[1]

> アイデンティティは相手との関係性（コンテキスト）の中で定義される「～としての自分」のことである。

[1] 出所：http://pii-desu.hp.infoseek.co.jp/erikuson.htm

プライバシーの尊重

「～としての自分」は、意識的・無意識的に、どのような情報を相手と共有するかを選んでいる。

> データ・情報の共有は、相手との関係性の中のような、あるコンテキストの中で行われている。

これは、相手との関係性の価値を高めようとする活動の中で行われている。プライバシーを尊重するということは、この関係性を尊重するということである。

> プライバシーの尊重とは、ある個人が保とうとしている関係性・コンテキストを尊重することである。

往々にして、このコンテキストの中からデータ・情報を外に取り出すと、その関係性は阻害される。これを、プライバシーの侵害という。

> あるコンテキストから、本人の同意なしにデータ・情報を取り出し、その関係性を損なうことをプライバシーの侵害という。

したがって、あるデータ・情報がプライバシーデータだというような主張は成り立たない。例えば、住所情報をとってみよう。自宅でビジネスをしている人にとっては、そのビジネスに伴って住所を広く知ってもらうことはメリットがあり、それを伝えることはプライバシーの侵害にはならない。一方、DVの被害者にとっては、住所を元の夫に知られることは死活問題になる。したがって、住所を公開されることはプライバシーの侵害となる。

> あるデータ・情報がプライバシー情報であるか否かは、その情報の種類によって規定されるのではなく、そのコンテキストによって規定される。

現在の日本の個人情報保護法を含む多くの個人情報保護法・条例は、どちらかというとデータ保護法としての側面が強く、プライバシー保護にはなっていないことが多い。プライバシー保護という側面は、データの種類によって決まる話ではなく、ケースバイケースで判断されなければならないことも多々ある。そのため、紛争時にはプライバシーコミッショナーによる裁定のようなものが求められることが多く想定される。諸外国と異なり、日本にはプライバシーコミッショナー制度が無い。今後、プライバシー保護法制の制定と共にコミッショナー制度の制定も求められると言えよう。

同意フレームワーク

したがって、プライバシーを尊重するには、あるデータを別の場所に移そうとするときに本人の同意をとることが必須となる。この同意をとる方法のことを、同意フレームワークという。

> 同意フレームワークとは、情報をあるコンテキストから他のコンテキストに移動する許可を本人から得るための技術的フレームワークのことを指す。

同意を得る際には、その同意が何を意味しているのかを本人が理解していることが重要である。この理解が十分でなく、誤解に基づいて同意してしまうことが往々にある。これを錯誤に基づく同意という。同意フレームワークにおいては、その同意が錯誤に基づくものでないことを確認することが重要である。

> 同意を得る際には、本人の理解が得られていることを確認し、それを後に証明できるような形で記録することが重要である。

逆に言えば、錯誤無効を主張されないためには、どのようなユーザーインターフェイスを持っているべきかということは、同意フレームワークの重要な検討課題である。

> 錯誤無効を産まないようなユーザーインターフェイスは同意フレームワークの重要課題である。

同意フレームワークとしての OpenID

同意は、対面（口頭）や書面でとることも可能であるが、インターネット上では、コンピュータや携帯電話上のユーザーインターフェイスを通して取得することが有効である。OpenID は、この同意をとるためのフレームワークである。

> OpenID は、データ提供の同意確認をとるための、フレームワークである。

インターネット上で同意をとるためには、以下の二つのプロセスを経なければならない。

1. 今まさに同意をしようとしているユーザーが、同意を与えうる本人であることの確認（本人確認）
2. データの内容、転送先、条件の、上記ユーザーによる確認（同意確認）

上記の 1. を「認証」、2. を「許可」と呼ぶことも多い。「OpenID は認証フレームワークである」としばしば巷間言われるが、これは、上記の 1. に注目した発言である。しかし、OpenID の本質は、1. 2.双方持っていることにある。

OpenID の流れは以下の図のようになる。

図1　OpenID のフロー

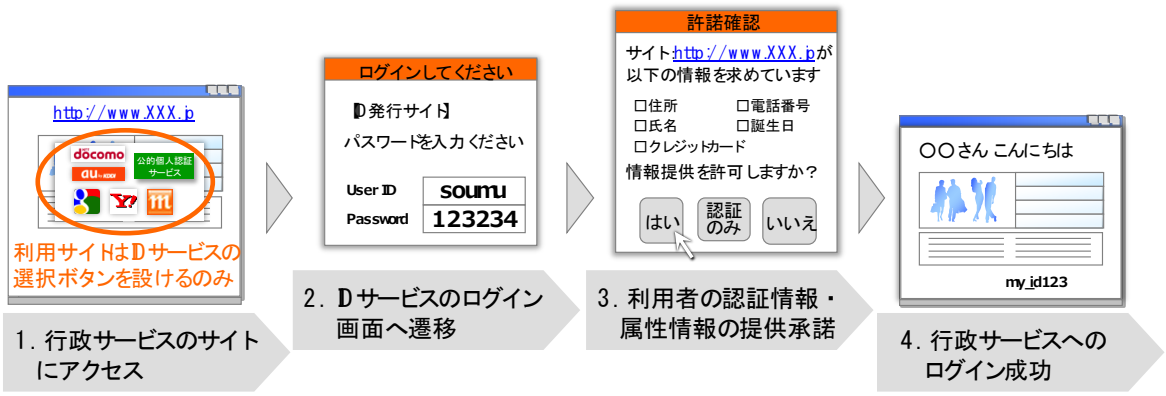


図2,3 は、日本航空において実際に利用されているホテル予約の画面である。これは、OpenID を使って、ホテル予約に必要な情報を実際に転送するにあたって、ユーザーに同意を求めている画面である。

図2 日本航空における認証画面

図3 JAL の OpenID でのデータ提供同意画面の例

このようにしてデータの提供が行われたさい、誰に、どのような条件で、いつ提供されたのかが記録されるべきである。（個人のレベルではほとんど管理不能であることが分かっている。）図3は、JAL

の提供情報管理画面である。

図4　提供情報管理画面

第三者提供アイデンティティ

OpenID において、認証を行うサーバーのことを、**Identity Provider (IdP)**ないし、**OpenID Provider (OP)** という。
IdP は、多くの場合、**属性情報**の提供も行う。
属性情報には「形質」「(狭義の)属性」「嗜好」「関係性」が含まれる。
形質とは、生年月日や性別、眼の色、指紋など、変わらないか、ゆっくりしか変化しないものである。
(狭義の)属性は、形質に比べ変化する速度が早いもので、代表的なものに電話番号、メールアドレスなどの識別子や、位置情報などがある。特殊なところでは、パスワードなども属性情報の一種である。
嗜好は、好きな食べ物、好きな音楽など、好みをあらわすものである。
関係性は、ある店舗の顧客としての関係や、友人関係などがある。昨今話題のソーシャルグラフもこの関係性に含まれる。

こうした情報を受け取るサーバーのことを、**Relying Party (RP)** という。直訳すれば、依存者である。これは、認証や属性を IdP に「依存」するからこのように呼ばれる。従来型の Web サービスなどでは、RP と IdP は一体であったが、OpenID のようなシステムでは、これが IdP と RP に分離している。このようなモデルを**「第三者提供アイデンティティ(Third Party Provided Identity)」**という。Third Party Provided Identity の代表例として、OpenID, SAML, Infocard, Kerberos などがある。

第三者提供アイデンティティ・モデルでは、IdP と呼ばれるサーバーが提供する認証やその他の属性情報を、RP と呼ばれるサーバーが受け取り、何らかのサービスを提供する。IdP と RP が同じ主体に管理されていれば、IdP が提供する情報の信頼度を RP は知っていると言える。しかし、異なる主体が提供している場合、一般的には、IdP が提供する情報がどの程度信頼できるのかを RP が知っているとは言えない。ここに、情報の非対称性が存在する。

同様に、RP が受け取った情報を適切に取り扱うと宣言していても、本当にそうかを知ることは、一般的には IdP もユーザー自身も知ることはできない。ここにも情報の非対称性が存在する。

> 第三者提供アイデンティティのモデルにおいては、ユーザー、IdP、RP 夫々において情報の非対称性が存在し、市場は効率的でない。したがって、この非対称性を緩和する政策が必要である。

この対策として代表的なものが、第三者監査制度である。この制度では、第三者が IdP、RP それぞれについて監査を行ない、その結果を公表することによって、本人申請ベースよりも格段に信頼度を上げるものである。こうしたものを、トラストフレームワークと呼ぶ。

トラスト・フレームワーク

このようにして、「第三者提供 ID」の利用を始めると、責任分界点の決定と、それを反映した契約を結ぶ必要が出てくる。これを個別にやると、対象の主体が N いると、N(N-1)/2 個という膨大な契約が必要になってしまう。これは明らかにスケールしない。これをスケールさせるためには、中心となる契約者一者と契約すれば、全体と契約を行った形になるようにして、必要な契約数を N 個に抑えるべきである。上記の「審査・認定」と、この「統一契約」はセットになるものであり、これを行う者を「トラスト・フレームワーク・プロバイダ」と言う。これを制度として設置しなければならない。

> トラスト・フレームワーク・プロバイダ制度を策定しなければならない。

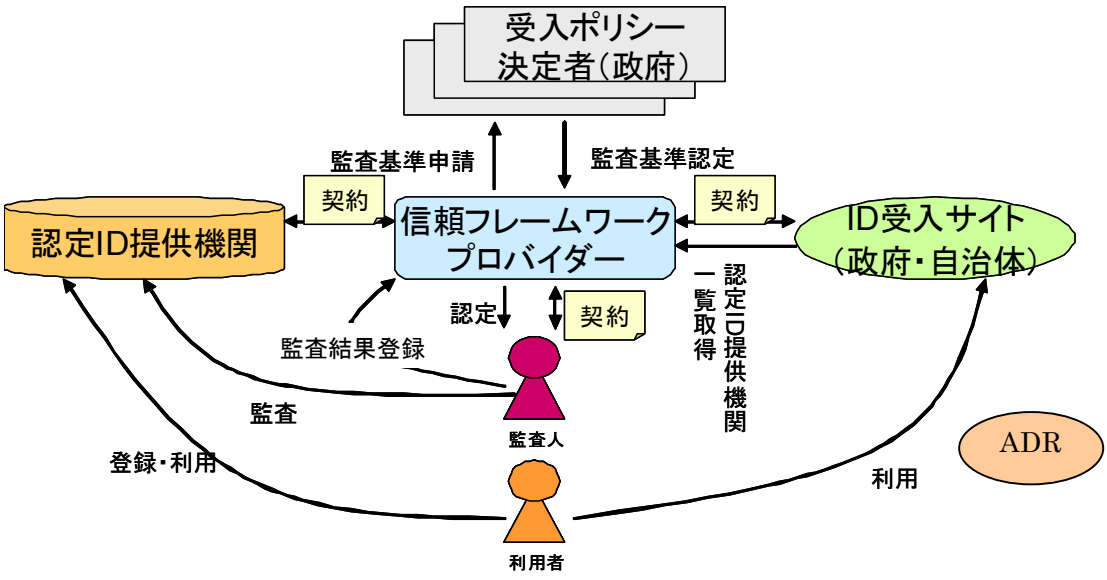
また、この制度のもと、各主体ともに、責任範囲を定め、その範囲での賠償責任があることを認め、実行しなければならない。

> トラスト・フレームワークで定められた契約に記載された責任分界点に従い、各主体同士で、相互に賠償責任を認め、実行しなければならない。

このようなトラスト・フレームワークの例としては、米国政府が推進している Open Identity Trust Framework（OITF）がある。具体的な検討の実施にあたっては、ゼロベースで行うよりも、これらの成果を最低限のカスタマイズによって使っていくことが、クロスボーダー時代・クラウド時代には相応しい、「ガラパゴス化・仲間はずれ化」しない方式であると言える。

> トラスト・フレームワークの検討にあたっては、米政府 OITF の例などを中心に、国際的な流れにできるだけ合致させ、クロスボーダー／クラウド時代に備えるべきである。

図5　米政府、OITF の例



法律は長年にわたり、社会の基盤をなしてきた。しかし、昨今の急速な技術進化や社会の変化に追随できなくなってきて、社会の基盤たるよりも社会の障害たるケースも散見されるようになってきていると、一部では認識されている。

この原因の一つとして、個別の技術などにあまりにも依存した形で立法が行われていることが多いということがある。たとえば、「印鑑」[2]というものは、日本の法令で多くの場所で用いられているが、現代においては技術的に完全に「危殆化」しており、証明能力は皆無である。にもかかわらず、法令に「印鑑」として指定してあるため、さまざまな課題を産んでしまっている。(そもそも、「印鑑」の定義は何か？)これは、本来立法時に「印鑑」を用いることによって達成しようとしていた目的を記述し、技術を記述しないことによって回避できた問題である。同様のことは、書証[3]に関しても言える。

こうしたことに鑑み、個別の技術を指定せずに目的ベースで記述し、かつ法や政府の介入を最小化し、法体系をインセンティブスキームを中心としたゲーム論的に再構成しようという考え方も存在する。

一般に、市場が効率的なとき、政府などの介入は資源配分を阻害し、全体の厚生を低下させることが知られている。したがって介入が許されるのは、市場が効率的でなくなる＝市場の失敗が生じている自体ということになる(厚生経済学の第一基本定理)。公平性の観点は、その後である。現代的な法体系を考える際には、こうした考え方も取り入れつつ行われる必要があろう。

2 印鑑の定義はどこでされているのだろうか？
3 書証や書類の定義はどこでされているのだろうか？

落穂拾い

識別子だけでは役に立たない

しばしば米国の SSN(Social Security Number)や韓国の住民登録番号を引き合いに出して、「番号(＝識別子の一種)」があれば効率化するというような議論がなされる。しかし、実際には、識別子だけがあったところで、その識別子を申請した人間が正当な人間であるかどうか(＝なりすまし等がないか)確認のしようがないので、ほとんど役に立たない。米国や韓国では多くの Identity Theft がこのせいで起きており、韓国では 2015 年までに住民登録番号のインターネット上での仕様を禁止、米国では 2006 年(？＝要確認)に原則使用が禁止されている。

個人情報保護法と条例

個人情報保護法は民間に対するものと、府省に対するものはあるが、自治体は個別の条例によっている。そのため、個人情報保護の内容は各自治体ごとに異なる。これは、データのやりとりにとって、大きな障害となっている。

ビジョンと民主主義

- 民主主義の基本としての情報公開
- 市民および民間非営利による監視
- 爆発するデータ量をさばくコンピュータ化された分析のための API
- Gov2.0

レピュテーション(評判情報)

- 監査は一時点のものである。連続した観察を反映するものとしては、レピュテーションのほうがふさわしい。